REMARKS

Reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks is respectfully requested.

Claims 1-19 are pending.

Claims 1-19 are patentable over *Moran* (U.S. Patent 6,647,400)

The rejection of claims 1-19 under 35 U.S.C. 102(e) as being anticipated by *Moran* is hereby traversed. A rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently. *Moran* fails to disclose all limitations of the claimed subject matter of claim 1 for at least three reasons.

First, *Moran* fails to disclose reading events representing various types of system calls. The PTO's reliance on column 7, line 65-column 8, line 23 and column 13, line 26-42 is noted; however, the cited portions of *Moran* fail to provide a disclosure of reading events representing various types of system calls. The cited passages are reproduced below for the PTO's convenience of review.

In particular, *Moran* describes in column 7, line 65-column 8, line 23 the following:

> A computer security system in accordance with the invention comprises an intrusion detection system capable of reviewing data and identifying and characterizing intrusions after the fact. The inventive system is capable of handling events that are seconds, days, weeks, or longer ago. The system is configured to collects evidence about an attack and to organize that evidence into an assessment of the attacker's actions and possible intent.
>
> The architecture of an embodiment of the inventive intrusion detection system is shown in FIG. 3. A user interface 300 on a console (FIG. 4 shows an exemplary display on the user interface 300) provides the system administrator with access to the analysis engine 302 and event database 304. Analysis engine 302 utilizes ruleset 306 and an attack signatures database 308, and receives input from sensor controller 310. The sensor controller 310 is in communication with various sensors (in the form of data collection modules) 312, and may pass information to the

> event database 304. For efficiency and ease of use, the sensor controller 310 may be combined with the sensors 312 into a single program or process, as shown by dotted box 314, but the sensors 312 may individually or collectively be run independently of the sensor controller 310. Although the architecture has been presented in terms of a specific embodiment, one skilled in the art will recognize that the various elements show may be combined in different ways, or further separated into other elements.

These paragraphs appear to describe how the sensors of *Moran* are arranged and connected to other components of the *Moran* system. However, the paragraph does not appear to teach or disclose whether the sensors read events representing various types of system calls.

Moran describes in column 13, lines 26-42, the following:

> In an embodiment of the invention, the analysis engine uses a declarative knowledge base. The specifications of what to look for are provided in a human-oriented format, the transformed and compiled into rules that allow the inventive system to respond efficiently to pieces of evidence as they arrive. Because some of the evidence of an attack will likely have been lost before the analysis engine is run, the specification of how to interpret evidence assigns four weights to each piece of evidence:
>
> 1. Likelihood that the underlying event is part of the larger sequence (e.g., is it a critical component, one of several alternatives, or something that routinely occurs).
> 2. Likelihood of finding the evidence.
> 3. Likelihood that the underlying event indicates that the larger sequence did not occur (i.e., it is contrary evidence).
> 4. Severity (cost of recovery/damage).

This paragraph appears to describe how the declarative knowledge base which *Moran* uses for an analysis engine operates. However, this paragraph fails to teach or disclose reading events representing various types of system calls as claimed. Although this cited portion of *Moran* does use the word event, there is no teaching or disclosure that the event represents various types of system calls. To the contrary, read as a whole, the cited portion suggests that the analysis engine operates on evidence resulting from an event occurrence and not that the analysis engine operates based on an event. For at least this reason, withdrawal of the rejection is respectfully requested.

Second, column 7, line 65-column 8, line 23 and column 14, lines 13-31 of *Moran*, fail to disclose routing an event to an appropriate template, the event having multiple parameters. Instead, column 7, line 65-column 8, line 23 of *Moran* appears to describe, as shown above, how the sensors of *Moran* are arranged and connected to other components of the *Moran* system. There is no disclosure of routing of an event to an appropriate template or that the event has multiple parameters.

Moran describes in column 14, lines 13-31, the following:

> In an embodiment of the invention, a wide range of data sources is used. To facilitate this, the inventive system's architecture comprises a set of mechanisms that allow additional data sources to be incorporated into the system. This set of mechanisms includes the following:
>
> an extensible family of communications protocol, based upon a meta-protocol;
>
> a declarative rule set to provide the analysis engine with a specification of the sensor for a data source. The rule set for a new sensor can be loaded into an already running analysis engine, which can then immediately start to utilize that sensor; and
>
> a declarative rule set specifying the interactions of the data from the new data source with that from other sources. Such rule sets can be incrementally added to an already running analysis engine. Rules that reference data sources not currently available to a particular analysis engine may be silently ignored (as moot).

This paragraph appears to describe the mechanisms of the *Moran* system for incorporating data sources into the system, i.e., a communications protocol, a declarative rule set for specification of sensor data, and a declarative rule set for specifying interactions of data. However, this paragraph fails to teach or disclose routing of an event to an appropriate template or that the event has multiple parameters. For at least this reason, withdrawal of the rejection is respectfully requested.

Third, *Moran* fails to disclose filtering an event as either a possible intrusion based on the multiple parameters and either dropping the event or outputting the event. The PTO's reliance on column 11, lines 15-65 and column 32, lines 48-59 of *Moran* is noted; however, the cited portions of *Moran* fail to provide a disclosure of the claim limitation. The cited passages are reproduced below for the PTO's convenience of review.

In particular, *Moran* describes in column 11, lines 15-65, the following:

> In an embodiment of the invention, the primary data source is the computer's filesystem, and multiple correlations are checked between files. Changes to system files and directories change infrequently and in largely predictable ways, attacks often leave a system directory in a state that is not only inconsistent with normal practice, but that is indicative of a particular class of attacks. This evidence is obtained by correlations between dates on the files and the directory, between dates on files and their relative order in the directory, and on dates of files relative to the information left in a directory when a file is deleted or removed.
>
> The inventive system may also search the filesystem, including deleted entries, for filenames and filename patterns that are known parts of attacks, such as names that are part of attack scripts in circulation or use, and names that are part of the standard operating practice/modus operandi of attackers. Filesystem information, both timestamps and file signatures, may be recovered from backup dumps without having to reload the files and directories to disk. In an embodiment of the invention, the system supports the ufs-dump format, which is the most commonly used on a range of UNIX systems, and supports additional dump formats with data collection modules as needed.
>
> Some of the programs most likely to be involved in an attack produce log entries for significant events. Some of these put related, often overlapping, information into different log files. There are commonly available hacker tools that help an attacker hide his tracks by deleting selected entries from these files, but these tools leave evidence of the deletion behind. Thus, the inventive system scans log files looking for evidence of an attack and for inconsistencies between the following:
>
> entries within each log file,
> related entries in different log files, and
> entries in the log file and information that is expected to be found within the filesystem (for example, between an user's login entries and his login start up files).
>
> Configuration-checking is an important part of securing a computer, and there are multiple research systems available (COPS-Computerized Oracle and Password System, Texas A&M University's Tiger) and subsequent commercial versions. The intrusion detection system of the invention includes a variety of checks on the computer system's configuration, but because of different circumstances and goals, it may use that information differently from configuration-checkers. For example, a typical configuration checker will produce pages of warnings about a vendor's baseline operating system installation.

This portion of *Moran* appears to describe date correlations performed between files and directories of a system to determine changes, searches for known filenames and filename patterns, comparing log file entries, and configuration checking. However, the paragraph does not appear to teach or disclose filtering an event based on multiple parameters and either dropping the event or outputting the event.

Moran describes in column 32, lines 48-59, the following:

> One check is to iterate through the files in the package management database, comparing the signatures in the database to the signature of the current version of the file. If the signatures match, the analysis engine draws no conclusion, because this provides no evidence to distinguish the two cases: (1) the file could be correct; or (2) the attacker has modified the database to have the signature of a file he installed. If there is a mismatch of signature, the analysis engine then checks if the mismatch is expected, and if not, the file is flagged as suspicious. Expected mismatches are determined by a set of rules:

This paragraph appears to describes cross checking files with signatures of current versions of the file in a database. However, the paragraph does not appear to teach or disclose the claimed limitation of filtering an event. For at least this reason, withdrawal of the rejection is respectfully requested.

Based on each of the foregoing reasons, claim 1 is patentable over *Moran* and the rejection is respectfully requested to be withdrawn.

Claims 2-6 and 13 depend, either directly or indirectly, from claim 1, include further limitations, and are patentable over *Moran* for at least the reasons advanced above with respect to claim 1. The rejection of claims 2-6 and 13 should be withdrawn.

Claim 7 is patentable over *Moran* for at least reasons similar to those advanced above with respect to claim 1 and withdrawal of the rejection is respectfully requested.

Claims 8-12 depend, either directly or indirectly, from claim 7, include further limitations, and are patentable over *Moran* for at least the reasons advanced above with respect to claim 7. The rejection of claims 8-12 should be withdrawn.

Claim 14 is patentable over *Moran* for at least reasons similar to those advanced above with respect to claim 1 and withdrawal of the rejection is respectfully requested.

Claims 15-19 depend, either directly or indirectly, from claim 14, include further limitations, and are patentable over *Moran* for at least the reasons advanced above with respect to claim 14. The rejection of claims 15-19 should be withdrawn.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,
Mark Crosbie et al.

Randy A. Noranbrock

Randy A. Noranbrock
Registration No. 42,940

Customer Number: 22879
Cathi Christensen
Hewlett-Packard Company
Legal Department MS 79
3404 E. Harmony Rd
Ft. Collins, CO 80528
(970) 898-4403
(970) 898-7247 facsimile
Date: **June 16, 2006**

RAN/cv/iyr